

# United States District Court

FOR THE  
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

FILED  
2016 MAY 31 P 4:09

SUSAN Y. SOONG  
CLERK, US DISTRICT COURT  
NO. DIST. OF CA.

UNITED STATES OF AMERICA,

V.

BTC-E, A/K/A CANTON BUSINESS CORPORATION,  
ANDREY NIKONOROV,  
STANISLAV GOLOVANOV,  
ALEXANDER BUYANOV, and  
ALEXANDER VINNIK.

SI

CR16

0227

DEFENDANT(S).

## INDICTMENT

18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business;  
18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering;  
18 U.S.C. § 982(a)(1) – Criminal Forfeiture

A true bill.



Foreman

Filed in open court this 31<sup>st</sup> day of

May, 2016

Clerk

Bail, \$

*no bail amount wanted for  
for individual defendants; no money for BTC-E  
Eugene D. Lepore*

AO 257 (Rev. 6/78)

**DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT**
 BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT  
☐ SUPERSEDING
**OFFENSE CHARGED**
 18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business; ☐ Petty  
 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering; ☐ Minor  
 18 U.S.C. § 982(a)(1) - Criminal Forfeiture ☐ Misdemeanor  
☒ Felony
**PENALTY:**
 5 years imprisonment for 18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business;  
 20 years imprisonment for 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering;

Name of District Court and Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - U.S.

BTC-E A/K/A CANTON BUSINESS CORPORATION

DISTRICT COURT NUMBER

CR16

0227

ST

**PROCEEDING**

Name of Complainant Agency, or Person (&amp; Title, if any)

Internal Revenue Services

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:

☐ U.S. ATTORNEY ☐ DEFENSE

SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

MAGISTRATE CASE NO.

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person

Furnishing Information on this form BRIAN STRETCH

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S.

Attorney (if assigned)

KATHRYN HAUN

**IS NOT IN CUSTODY**

Has not been arrested, pending outcome this proceeding.

- 1) ☒ If not detained give date any prior summons was served on above charges
- 2) ☐ Is a Fugitive
- 3) ☐ Is on Bail or Release from (show District)

**IS IN CUSTODY**

- 4) ☐ On this charge
- 5) ☐ On another conviction } ☐ Federal ☐ State
- 6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

 Has detainer been filed? ☐ Yes ☐ No

If "Yes" give date filed

DATE OF ARREST

Month/Day/Year

Or... if Arresting Agency &amp; Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY

Month/Day/Year

☐ This report amends AO 257 previously submitted
**ADDITIONAL INFORMATION OR COMMENTS****PROCESS:**
☐ SUMMONS ☐ NO PROCESS\* ☒ WARRANT

Bail Amount: \_\_\_\_\_

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address: \_\_\_\_\_

\* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Date/Time: \_\_\_\_\_ Before Judge: \_\_\_\_\_

Comments: \_\_\_\_\_

## DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT  
☐ SUPERSEDING

## OFFENSE CHARGED

18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business;  
 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering;  
 18 U.S.C. § 982(a)(1) - Criminal Forfeiture

☐ Petty  
☐ Minor  
☐ Misdemeanor  
☒ Felony

## PENALTY:

5 years imprisonment for 18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business;  
 20 years imprisonment for 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering;

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - U.S.

ANDREY NIKONOROV

DISTRICT COURT NUMBER

CR16

0227

## PROCEEDING

Name of Complainant Agency, or Person (&amp; Title, if any)

Internal Revenue Services

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:

☐ U.S. ATTORNEY ☐ DEFENSE

SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

MAGISTRATE CASE NO.

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person

Furnishing Information on this form BRIAN STRETCH

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned)

KATHRYN HAUN

## IS NOT IN CUSTODY

Has not been arrested, pending outcome this proceeding.

1) ☒ If not detained give date any prior summons was served on above charges

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

## IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction

☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☐ No

If "Yes" give date filed

DATE OF ARREST

Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY

Month/Day/Year

☐ This report amends AO 257 previously submitted

## ADDITIONAL INFORMATION OR COMMENTS

## PROCESS:

☐ SUMMONS ☐ NO PROCESS\* ☒ WARRANT

Bail Amount: \_\_\_\_\_

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

Date/Time: \_\_\_\_\_

Before Judge: \_\_\_\_\_

Comments:

\* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

AO 257 (Rev. 6/78)

**DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT**
 BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT  
☐ SUPERSEDING
**OFFENSE CHARGED**

18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business;

18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering;

18 U.S.C. § 982(a)(1) – Criminal Forfeiture

☐ Petty  
☐ Minor  
☐ Misdemeanor  
☒ Felony
**PENALTY:**
 5 years imprisonment for 18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business;  
 20 years imprisonment for 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering;

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - **US**

STANISLAV GOLOVANOV

DISTRICT COURT NUMBER

**DEFENDANT****IS NOT IN CUSTODY**

Has not been arrested, pending outcome this proceeding.

- 1) ☒ If not detained give date any prior summons was served on above charges
- 2) ☐ Is a Fugitive
- 3) ☐ Is on Bail or Release from (show District)

**IS IN CUSTODY**

- 4) ☐ On this charge
- 5) ☐ On another conviction } ☐ Federal ☐ State
- 6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution                     
 Has detainer ☐ Yes  
 been filed? ☐ No

 If "Yes"  
 give date  
 filed                     
**DATE OF ARREST**Month/Day/Year                     

Or... if Arresting Agency &amp; Warrant were not

**DATE TRANSFERRED TO U.S. CUSTODY**Month/Day/Year                     ☐ This report amends AO 257 previously submitted**PROCEEDING**

Name of Complainant Agency, or Person (&amp; Title, if any)

Internal Revenue Services

☐ person is awaiting trial in another Federal or State Court, give name of court                     
☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District                     
☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:

☐ U.S. ATTORNEY ☐ DEFENSE
SHOW DOCKET NO.                     
☐ this prosecution relates to a pending case involving this same defendant
MAGISTRATE CASE NO.                     
☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under                     

Name and Office of Person

Furnishing Information on this form BRIAN STRETCH☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned)

KATHRYN HAUN**ADDITIONAL INFORMATION OR COMMENTS****PROCESS:**☐ SUMMONS ☐ NO PROCESS\* ☒ WARRANTBail Amount:                     

If Summons, complete following:

☐ Arraignment ☐ Initial AppearanceDefendant Address:                     

\* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Date/Time:                      Before Judge:                     Comments:



# DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT  
☐ SUPERSEDING

## OFFENSE CHARGED

18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business;

18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering;

18 U.S.C. § 982(a)(1) – Criminal Forfeiture

☐ Petty

☐ Minor

☐ Misdemeanor

☒ Felony

## PENALTY:

5 years imprisonment for 18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business;  
 20 years imprisonment for 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering;

Name of District Court and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT - U.S.

ALEXANDER BUYANOV

DISTRICT COURT NUMBER

CR16

0227

## PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)

Internal Revenue Services

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:

☐ U.S. ATTORNEY ☐ DEFENSE

SHOW  
DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

MAGISTRATE  
CASE NO.

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person

Furnishing Information on this form BRIAN STRETCH

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S.

Attorney (if assigned)

KATHRYN HAUN

## DEFENDANT

### IS NOT IN CUSTODY

Has not been arrested, pending outcome this proceeding.

1) ☒ If not detained give date any prior summons was served on above charges

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

### IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction

☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☐ No

If "Yes" give date filed

DATE OF  
ARREST

Month/Day/Year

Or... if Arresting Agency & Warrant were not

DATE TRANSFERRED  
TO U.S. CUSTODY

Month/Day/Year

☐ This report amends AO 257 previously submitted

## ADDITIONAL INFORMATION OR COMMENTS

### PROCESS:

☐ SUMMONS ☐ NO PROCESS\* ☒ WARRANT

Bail Amount: \_\_\_\_\_

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

\* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Date/Time: \_\_\_\_\_ Before Judge: \_\_\_\_\_

Comments:

AO 257 (Rev. 6/78)

**DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT**
 BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT  
☐ SUPERSEDING
**OFFENSE CHARGED**
 18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business; ☐ Petty  
 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering; ☐ Minor  
 18 U.S.C. § 982(a)(1) – Criminal Forfeiture ☐ Misdemeanor  
☒ Felony
**PENALTY:**
 5 years imprisonment for 18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business;  
 20 years imprisonment for 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering;

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

DEFENDANT: U.S.

ALEXANDER VINNIK

DISTRICT COURT NUMBER

CR16

0227

**PROCEEDING**

Name of Complainant Agency, or Person (&amp; Title, if any)

Internal Revenue Services

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrP 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of:

☐ U.S. ATTORNEY ☐ DEFENSE
SHOW  
DOCKET NO.
☐ this prosecution relates to a pending case involving this same defendant
MAGISTRATE  
CASE NO.
☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under

Name and Office of Person

Furnishing Information on this form BRIAN STRETCH

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S.

Attorney (if assigned)

KATHRYN HAUN

**IS NOT IN CUSTODY**

Has not been arrested, pending outcome this proceeding.

 1) ☒ If not detained give date any prior summons was served on above charges
2) ☐ Is a Fugitive3) ☐ Is on Bail or Release from (show District)**IS IN CUSTODY**4) ☐ On this charge5) ☐ On another conviction
☐ Federal ☐ State
6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

 Has detainer been filed? ☐ Yes ☐ No

If "Yes" give date filed

DATE OF  
ARREST

Month/Day/Year

Or... if Arresting Agency &amp; Warrant were not

DATE TRANSFERRED  
TO U.S. CUSTODY

Month/Day/Year

☐ This report amends AO 257 previously submitted
**ADDITIONAL INFORMATION OR COMMENTS****PROCESS:**
☐ SUMMONS ☐ NO PROCESS\* ☒ WARRANT

Bail Amount: \_\_\_\_\_

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

\* Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment

Date/Time: \_\_\_\_\_

Before Judge: \_\_\_\_\_

Comments:

BRIAN J. STRETCH (CABN 163973)  
United States Attorney

FILED

2016 MAY 31 P 4:10

SUSAN Y. SOONG  
CLERK, US DISTRICT COURT  
NO. DIST. OF CA.

SEALED BY ORDER  
OF COURT

SI

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

BTC-E, A/K/A CANTON BUSINESS  
CORPORATION,  
ANDREY NIKONOROV,  
STANISLAV GOLOVANOV,  
ALEXANDER BUYANOV, and  
ALEXANDER VINNIK.

Defendants.

UNDER SEAL

CASE NO.

**CR16 0227**  
VIOLATIONS: 18 U.S.C. § 1960 – Operation of an  
Unlicensed Money Service Business; 18 U.S.C.  
§ 1956(h) – Conspiracy to Commit Money  
Laundering; 18 U.S.C. § 982(a)(1) – Criminal  
Forfeiture

SAN FRANCISCO VENUE

INDICTMENT

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this Indictment:

1. Since at least approximately 2011 through and including the present, both dates being approximate and inclusive, the defendants engaged in the operation and running of BTC-e, one of the world's largest and most widely used digital currency exchanges. Since its inception, it processed several billion dollars worth of monetary exchanges. BTC-e was an exchange for cybercriminals worldwide, and one of the principal entities used to launder and liquidate criminal proceeds between

1 digital currencies, including Bitcoin, to fiat currencies,<sup>1</sup> including U.S. dollars, Euros, and Rubles.

2       2.       BTC-e was an international money-laundering scheme that, by virtue of its business  
3 model, catered to criminals – and to cybercriminals in particular. It facilitated crimes, including  
4 computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption,  
5 and drug trafficking.  
6

7       3.       BTC-e lacked basic anti-money laundering controls and policies and, as such, was  
8 attractive to those who desired to conceal criminal proceeds as it made it more difficult for law  
9 enforcement to trace and attribute funds.

10       4.       Since its founding, BTC-e received criminal proceeds of numerous computer intrusions  
11 and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics  
12 distribution rings. Among other things, BTC-e accounts received substantial proceeds from the hack of  
13 the now-defunct Mt. Gox digital currency exchange and also received a substantial portion of the  
14 criminal proceeds from one of the largest ransomware schemes, CryptoWall.  
15

16       5.       As described further below, the defendants and their co-conspirators, including those  
17 known and unknown to the Grand Jury, intentionally created, structured, and operated BTC-e as a  
18 criminal business venture, one designed to help criminals launder their proceeds and one they  
19 themselves used to launder criminal proceeds. The defendants thus attracted and maintained a customer  
20 base that was heavily reliant on criminals.  
21

22       6.       Despite doing substantial business in the United States, BTC-e was not registered as a  
23 money services business with the United States Department of the Treasury's Financial Crimes  
24 Enforcement Network ("FinCEN"), as federal law requires. As described further below, BTC-e had no  
25 meaningful anti-money laundering processes in place and lacked an effective anti-money laundering  
26

---

27       <sup>1</sup> Fiat currency is simply a currency established by government regulation or law, e.g. U.S.  
28 Dollars, Euros, Japanese Yen, British Pounds, Russian Rubles, Chinese RMB, etc.



1 program, as federal law also requires.

2 7. This was in contrast to other registered digital currency exchanges that, through their  
3 anti-money laundering programs, strove to avoid having their platforms used for criminal activity. Most  
4 of those exchanges described their operations down to listing the names, photos, and backgrounds of  
5 their management, the location of their businesses, and their regulatory compliance policies.

6 8. BTC-e relied on the use of shell companies and affiliate entities that were similarly  
7 unregistered with FinCEN and lacked basic anti-money laundering and “Know Your Customer”  
8 policies. These entities catered to an online and worldwide customer base, and electronically “muled”  
9 fiat currency in and out of BTC-e. BTC-e’s own website stated it was located in Bulgaria, yet  
10 simultaneously stated it was subject to the laws of Cyprus. Meanwhile, BTC-e’s managing shell  
11 company, CANTON BUSINESS CORPORATION, was based in the Seychelles but affiliated with a  
12 Russian phone number, and its web domains were registered to shell companies in countries including  
13 Singapore, the British Virgin Islands, France, and New Zealand.  
14  
15

#### 16 BACKGROUND

17 9. Bitcoin is a form of decentralized, convertible digital currency that existed through the  
18 use of an online, decentralized ledger system.<sup>2</sup> Bitcoin is just one of many forms of digital currency.  
19 There are many others, including litecoin, ethers, worldcoin, and dogecoin. However, bitcoin has the  
20 largest market capitalization of any present form of decentralized digital currency.

21 10. While bitcoin mainly exists as an Internet-based form of currency, it is possible to “print  
22 out” the necessary information and exchange bitcoin via physical medium. The currency is not issued  
23 by any government, bank, or company, but rather is generated and controlled through computer software  
24 operating via a decentralized network. To acquire bitcoin, a typical user will purchase them from a  
25 Bitcoin seller or “exchanger.” It is also possible to “mine” bitcoin by verifying other users’ transactions.  
26

27  
28 <sup>2</sup> Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the currency. That practice is adopted here.

1 Bitcoin is just one form of digital currency, and there are a significant number of other varieties of  
2 digital currency.

3 11. Bitcoin exchangers typically accept payments of fiat currency (currency which derives its  
4 value from government regulation or law), or other convertible digital currencies. When a user wishes  
5 to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency,  
6 often via bank wire or ACH, or other convertible digital currency to an exchanger, for the corresponding  
7 quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will  
8 then typically attempt to broker the purchase with another user of the exchange that is trying to sell  
9 bitcoin, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a  
10 seller, then the transaction can be completed.

11 12. When a user acquires bitcoin, ownership of the bitcoin is transferred to the user's bitcoin  
12 address. The bitcoin address is somewhat analogous to a bank account number, and is comprised of a  
13 case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can  
14 then conduct transactions with other Bitcoin users, by transferring bitcoin to their bitcoin addresses, via  
15 the Internet.

16 13. Little to no personally identifiable information about the payer or payee is transmitted in  
17 a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public  
18 key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address.  
19 Only the bitcoin address of the receiving party and the sender's private key are needed to complete the  
20 transaction. These two keys by themselves rarely reflect any identifying information.

21 14. All bitcoin transactions are recorded on what is known as the blockchain. This is  
22 essentially a distributed public ledger that keeps track of all bitcoin transactions, incoming and outgoing,  
23 and updates approximately six times per hour. The blockchain records every bitcoin address that has  
24 ever received a bitcoin and maintains records of every transaction for each bitcoin address.

25 15. Digital currencies, including Bitcoin, have many known legitimate uses. However, much  
26 like cash, Bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds, given the  
27 ease with which Bitcoin can be used to move funds with high levels of anonymity. As is demonstrated  
28 herein, however, in some circumstances Bitcoin payments may be effectively traced by analyzing the

1 blockchain.

2 ENTITIES AND INDIVIDUALS

3 16. As described further below, BTC-e's money laundering operation was partially enabled  
4 and supported by MAYZUS FINANCIAL LTD. a/k/a MAYZUS INVESTMENT COMPANY  
5 ("MAYZUS"). MAYZUS enabled a mechanism of moving money internationally centered principally  
6 on a core of companies owned by a Russian national. MAYZUS used to be known as UWC  
7 FINANCIAL SERVICES ("UWC"), but following the seizure and shuttering of another digital currency  
8 exchange, Liberty Reserve, UWC rebranded itself as MAYZUS FINANCIAL LTD.

9 17. MAYZUS offered a wide range of currency exchange services and provided the ability  
10 for fiat currency to be sent – through two online affiliates – to and from BTC-e. BTC-e utilized  
11 MAYZUS in lieu of a bank account.

12 18. MONEY POLO was an online payments system and affiliate of MAYZUS. MONEY  
13 POLO was registered in the British Virgin Islands with ties to Cyprus. In order to fund a MONEY  
14 POLO account, a user transferred funds to MAYZUS for the benefit of a specific MONEY POLO  
15 account number. A MONEY POLO account, in turn, was one of the mechanisms that could be used to  
16 fund a BTC-e account.

17 19. MAYZUS and MONEY POLO enabled BTC-e's operation and its business. Like BTC-  
18 e, neither MAYZUS nor MONEY POLO was registered as money service businesses with the United  
19 States Department of the Treasury's Financial Crimes Enforcement Network (FinCEN). In or about  
20 March 2016, Cyprus's Securities and Exchange Commission fined MAYZUS in connection with legal  
21 and regulatory violations stemming from lax anti-money laundering policies.

22 20. CANTON BUSINESS CORPORATION ("CANTON") was a shell corporation used as a  
23 front for BTC-e's operations. Like BTC-e, CANTON was not registered with FinCEN. Financial and  
24 other records demonstrate that CANTON was synonymous with BTC-e. The primary beneficial owners  
25 of CANTON's financial accounts were defendants ALEXANDER BUYANOV, STANISLAV  
26  
27  
28

1 GOLOVANOV, and ALEXANDER VINNIK. Although CANTON's listed business address was in the  
2 Seychelles, it operated using a Russian telephone number.

3 21. Defendant ANDREY NIKONOROV ("NIKONOROV"), a Russian national, was  
4 involved in the administration and operation of BTC-e and received substantial financial benefit from its  
5 continued operation. NIKONOROV also exercised control over and claimed ownership of a BTC-e  
6 account, known as the "Vamnedam"<sup>3</sup> account. This account was funded largely by proceeds from well-  
7 known hacks and thefts from bitcoin exchanges and users around the world. The "Vamnedam" account  
8 was also directly linked to the BTC-e administrative, financial, operational and support accounts,  
9 accounts to which only those involved in the operations of the BTC-e enterprise would have had access.  
10 Out of the Vamnedam account, payments of hundreds of thousands of dollars were made to  
11 NIKONOROV, and his co-defendants ALEXANDER BUYANOV and STANISLAV GOLONANOV.  
12

13 22. Defendant STANISLAV GOLOVANOV ("GOLOVANOV"), a Russian national, was  
14 also involved in administration and operation of BTC-e and received substantial financial benefit from  
15 its continued operation. GOLOVANOV has claimed ownership of CANTON BUSINESS  
16 CORPORATION, which as discussed above is a shell corporation for BTC-e. Like his co-defendants,  
17 GOLOVANOV is one of CANTON's primary beneficial owners.  
18

19 23. Defendant ALEXANDER BUYANOV ("BUYANOV"), a Russian national, was also  
20 involved in the administration and operation of BTC-e and received substantial financial benefit from its  
21 continued operation. Like his co-defendants, BUYANOV was also one of CANTON's primary  
22 beneficial owners. BUYANOV was also the registrant for BTC-e's websites, the account holder for its  
23 servers, and the account holder for a company that provided BTC-e with security and content  
24 distribution services.  
25

26 24. Defendant ALEXANDER VINNIK ("VINNIK"), a Russian national, was involved in the  
27

28 <sup>3</sup> Vamnedam means "I will not give it to you" in Russian.



1 administration and management of BTC-e. Like his co-defendants, VINNIK was also one of  
2 CANTON's primary beneficial owners. VINNIK, together with others known and unknown to the  
3 Grand Jury, controlled a BTC-e account known as the "WME" account, which was tied directly to BTC-  
4 e administrator accounts. Numerous withdrawals from BTC-e administrator accounts went directly to  
5 VINNIK's personal bank accounts.

#### 7 BTC-E OVERVIEW

8 25. BTC-e was founded in or about 2011. In the years it operated, BTC-e has served  
9 approximately 700,000 users worldwide, including numerous customers in the United States and  
10 customers in the Northern District of California. BTC-e touts itself as "a platform for individuals  
11 interested in buying and selling bitcoin using an assortment of world currencies;" in other words, a  
12 digital currency exchange.

13 26. Through the defendants and their work, BTC-e became one of the primary ways by  
14 which cybercriminals around the world transferred, laundered, and stored the criminal proceeds of their  
15 illegal activities. U.S. dollars and Russian rubles were the most frequently exchanged fiat currencies on  
16 the platform, while Bitcoin and litecoin were the most widely exchanged digital currencies.

17 27. Because such a significant portion of BTC-e's business was derived from suspected  
18 criminal activity and given its global reach, the scope of the defendants' unlawful conduct was massive.  
19 During the relevant timeframe from 2011 to 2016, BTC-e processed approximately 7.3 million bitcoin  
20 worth of deposits and approximately 5.5 million bitcoin worth of withdrawals. It is difficult to assign  
21 this a dollar value because of the fluctuating value of bitcoin and depending on when the deposit or  
22 withdrawal was made. However, using today's bitcoin exchange rate, BTC-e's total deposits would be  
23 valued at approximately \$3.8 billion and its withdrawals at approximately \$2.9 billion.<sup>4</sup>

---

24 <sup>4</sup> This is calculated using today's value of approximately \$532 per bitcoin. Bitcoin's market  
25 price has fluctuated as low as approximately \$4 per coin and as high as approximately \$1200 per coin,  
26 and has varied dramatically over time.

27 If those figures are instead measured when bitcoin reached its peak price in 2013, when a single  
28

1           28.     Notably, the above figures only include bitcoin exchanged on the BTC-e platform and do  
2 not even include the deposits and withdrawals made in other digital currencies, such as litecoin, nor do  
3 these figures take into account well over a billion dollars' worth of what is known as "BTC-e code."  
4 BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital currencies to other  
5 BTC-e users.

6  
7           29.     BTC-e maintained its servers in the United States. The servers were one of the primary  
8 ways in which BTC-e and the defendants effectuated their operations. BTC-e also used many third-  
9 party companies, including companies within the Northern District of California, to effectuate their  
10 operations and enable them to function.

11           30.     At its inception, BTC-e was one of a number of digital currency exchanges. It was  
12 engaged in the same line of business as other online digital currency exchanges in existence at the time,  
13 including Liberty Reserve. Liberty Reserve was a Costa Rica-based centralized digital currency service  
14 that laundered approximately \$6 billion in criminal proceeds. It was shuttered in 2013 when its founder  
15 and six other individuals were charged with conspiracy to commit money laundering and with operating  
16 an unlicensed money transmitting business. Liberty Reserve's website was seized by the U.S.  
17 government.<sup>5</sup>

18  
19           31.     There was an overlap between many Liberty Reserve users and BTC-e users. BTC-e  
20 itself was a user of Liberty Reserve, as was defendant GOLOVANOV, who used Liberty Reserve to  
21 conduct approximately \$5.6 million worth of transactions.

22  
23           32.     Another digital currency exchange in operation between 2011 and 2014 was the MTGOX  
24 Exchange ("Mt. Gox") that was originally founded in San Francisco, but ultimately based in Tokyo,  
25 bitcoin was worth over \$1200 per coin, the deposits and withdrawals would have been worth  
26 approximately \$8.4 billion and \$6.6 billion, respectively. On the flip side, if those figures are measured  
27 when BTC-e launched in 2011, when a single bitcoin was worth approximately \$10 per bitcoin, the  
deposits and withdrawals would have been worth approximately \$73 million and \$55 million,  
respectively.

28           <sup>5</sup> MAYZUS, through its predecessor, UWC FINANCIAL SERVICES, also served as an  
exchanger for Liberty Reserve.

1 Japan. In 2014, Mt. Gox collapsed, having been the target of a series of major intrusions that resulted in  
2 thefts totaling several hundred million dollars worth of bitcoin. In 2014, Mt. Gox filed for bankruptcy in  
3 Japan.

4 33. After the collapse of Liberty Reserve, and with the intrusions and accompanying issues  
5 that Mt. Gox experienced, BTC-e rapidly grew. The volume of transactions it performed and its number  
6 of users expanded, filling the vacuum left by entities like Liberty Reserve and Mt. Gox.  
7

#### 8 BTC-E FUNCTION

9 34. To use BTC-e, one created an account by accessing the BTC-e website. A user did not  
10 need to provide even the most basic identifying information such as name, date of birth, address, or  
11 other identifiers. All that BTC-e required was a username, password, and an email address. Unlike  
12 legitimate payment processors or digital currency exchangers, BTC-e did not require its users to validate  
13 their identity information by providing official identification documents, given that BTC-e did not  
14 require an identity at all.  
15

16 35. Thus, a user could create a BTC-e account with nothing more than a username and email  
17 address, which often bore no relationship to the identity of the actual user. Accounts were therefore  
18 easily opened anonymously, including by customers in the United States within the Northern District of  
19 California.  
20

21 36. At all times relevant to this Indictment, BTC-e had no anti-money laundering and/or  
22 “Know-Your-Customer” (KYC) processes and policies in place. As discussed above, BTC-e collected  
23 virtually no customer data at all. Nor did BTC-e or its shell companies ever register with FinCEN or  
24 perform these functions on BTC-e’s behalf.

25 37. A user could fund a BTC-e account in numerous different ways. One way involved  
26 funding the account with fiat currency that would be converted into digital currency, such as bitcoin.  
27 With fiat currency, a user could initiate a wire transfer from a financial institution made directly for the  
28

benefit of BTC-e to an account at another financial institution, which was routed to a bank account maintained by one of BTC-e's shell or affiliated companies. A BTC-e user could also fund an account through the use of a third-party payment system, like MONEY POLO, a third-party entity that maintained a direct relationship with BTC-e. MONEY POLO accounts worked to electronically "mule" fiat currency in and out of BTC-e. Incoming fiat currency was deposited into MAYZUS accounts (using its subsidiary MONEY POLO) to transfer into BTC-e. Outgoing digital currency was exchanged and converted to fiat currency and sent through MONEY POLO accounts benefiting MAYZUS.

38. Another way involved funding a BTC-e account with a user's existing digital currency. A user with existing digital currency, such as bitcoin, could fund a BTC-e account directly via bitcoin deposits. BTC-e users could also purchase "BTC-e code" that could be sent and exchanged amongst BTC-e users. BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital currencies to other BTC-e users. This served as another conduit for money laundering as it allowed BTC-e customers to withdraw funds from their BTC-e account and transfer them to other BTC-e users anonymously.

39. BTC-e's business model obscured and anonymized transactions and source of funds. For example, a BTC-e user could not fund an account by directly transferring money to BTC-e itself, but rather had to wire funds to one of BTC-e's shells or affiliate entities. Nor could BTC-e users withdraw funds from their accounts directly, such as through an ATM withdrawal. Instead, BTC-e users were required to make any deposits or withdrawals through the use of third-party "exchangers," thus enabling BTC-e to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail.

40. Once a user funded an account with BTC-e, the user could then do any number of things: conduct transactions with other BTC-e users; exchange digital currency into fiat currency; or simply use BTC-e to store digital currency deposits, much like a bank.

41. Like other digital currency exchanges, BTC-e charged transaction fees for their services.



1 BTC-e charged a percentage fee every time a user transferred funds held in BTC-e to another user  
2 through the BTC-e system. In addition, BTC-e charged a percentage fee every time a user used BTC-e  
3 to exchange digital currency held in a BTC-e account into fiat currency.<sup>6</sup> BTC-e's fees and percentages  
4 were higher than those charged by other exchanges that complied with the registration and anti-money  
5 laundering laws for comparable services.

6  
7 42. In addition to the fees BTC-e charged, users were charged additional fees by MONEY  
8 POLO and MAYZUS, each taking a percentage of the funds exchanged. These added fees were  
9 associated with getting money in and out of the BTC-e platform through these funding mechanisms,  
10 mechanisms that obfuscated the true sender of the currency.

11 43. Those engaged in criminal activity using BTC-e were willing to pay these higher  
12 percentages and additional fees, however, in exchange for knowing that BTC-e did not have anti-money  
13 laundering and "Know-Your-Customer" processes in place that could have them reported to the  
14 government. Criminals who used BTC-e to launder funds were also willing to go to the extra trouble of  
15 wiring money offshore to entities that operated through shell companies.

16  
17 44. BTC-e made a series of self-serving public statements, designed at least in part to deflect  
18 the attention of law enforcement and regulators. For example, despite advertising on their website that  
19 "[w]e require our clients to verify identity by providing [sic] scanned copy of ID and scanned copy of  
20 utility bill or a bank statement which should not be older then [sic] 6 month. Copy should be in good  
21 resolution and colored," this process was not in fact followed. As discussed, no customer identification  
22 whatsoever was required to set up BTC-e accounts, including BTC-e accounts set up by customers in the  
23 Northern District of California.

24  
25 45. Likewise, the BTC-e website advertised that "[w]e don't accept any more international  
26 wire transfers from US Citizens or from US Bank." This, too, was false. Through its elaborate funding  
27

28 <sup>6</sup> Likewise, MONEY POLO charged fees in addition to BTC-e's fees when transferring fiat currency in and out of BTC-e.

1 mechanisms, BTC-e did in fact knowingly accept wire transfers from banks in the U.S. and made by  
2 U.S. citizens.

3 BTC-E'S CRIMINAL DESIGN

4 46. As described above, BTC-e's system was designed so that criminals could accomplish  
5 financial transactions under anonymity and thereby avoid apprehension by law enforcement or seizure  
6 of funds. This was one of the reasons that BTC-e was able to charge higher fees for its exchange  
7 services than other, legitimate and registered digital currency exchangers who registered with FinCEN  
8 and who had appropriate and effective anti-money laundering and "Know-Your-Customer" policies in  
9 place.  
10

11 47. BTC-e was in fact thus used extensively for illegal purposes, and, particularly since the  
12 collapse of entities like Mt. Gox and Liberty Reserve, it functioned as the exchange of choice to convert  
13 digital currency like bitcoin to fiat currency for the criminal world, especially by those who committed  
14 their crimes online.  
15

16 48. The defendants were aware that BTC-e functioned as a money laundering enterprise.  
17 Messages on its own forum openly and explicitly reflected some of the criminal activity in which the  
18 users on the platform were engaged, and how they used BTC-e to launder funds.

19 49. BTC-e users established accounts under monikers suggestive of criminality, including  
20 monikers such as "ISIS," "CocaineCowboys," "blackhathackers," "dzkillerhacker," and "hacker4hire."  
21

22 50. This is not surprising because criminals used BTC-e to launder criminal proceeds and  
23 transfer funds among criminal associates. In particular, it was used by hacking and computer intrusion  
24 rings operating around the world to distribute criminal proceeds of their endeavors. It was also used by  
25 rings of identity thieves, corrupt public officials, narcotics distribution networks, and other criminals.

26 51. In fact, some of the largest known purveyors of ransomware used BTC-e as a means of  
27 storing, distributing, and laundering their criminal proceeds. Ransomware is a practice in which  
28

1 cybercriminals orchestrate the unwanted malicious download of encryption software on an unsuspecting  
2 victim computer. It works as follows: once a victim is infected with the malicious software, often by  
3 clicking on a fraudulent email, the ransomware will encrypt multiple files types on victim machines and  
4 hold those files for ransom, requiring the victim to pay the administrators of the ransomware scheme in  
5 order to have their files decrypted. Victims that pay the ransom are able to decrypt their files by using a  
6 stand-alone program provided by the ransomware administrators after the ransom payment has been  
7 made. The method of encryption implemented by the ransomware, if properly executed, renders it  
8 impossible for victims to decrypt their encrypted files in any other way. The only payment method  
9 accepted by purveyors of ransomware is bitcoin and other forms of digital currency.  
10

11         52. One such ransomware scheme, CryptoWall, was distributed by methods including  
12 fraudulent and phishing emails. CryptoWall was one of the most infamous varieties of ransomware and  
13 has infected countless computers across the world. During the timeframe relevant to this Indictment, the  
14 purveyors of CryptoWall deposited and laundered many hundreds of thousands of dollars' worth of  
15 ransom payments into BTC-e.  
16

17         53. So, too, did a pair of corrupt U.S. federal agents, Carl Mark Force and Shaun Bridges, use  
18 BTC-e to launder their criminal proceeds. Their experience with the criminal underworld taught them  
19 that using BTC-e, as opposed to a registered exchange with anti-money laundering policies, would  
20 maximize their chances of being able to conceal criminal proceeds. Each therefore sent several hundred  
21 thousand dollars in criminal proceeds – derived from crimes ranging from theft of government property  
22 to extortion – to the BTC-e platform for laundering.  
23

24         54. BTC-e also served as the receptacle and transmitter of criminal funds from a series of  
25 well-publicized computer intrusions and resulting thefts, including the well-publicized thefts from the  
26 Japan-based Mt. Gox exchange. As discussed below, a sizable portion of the stolen Mt. Gox funds were  
27 deposited into accounts controlled, owned, and operated by BTC-e and by defendants NIKONOROV,  
28

1 GOLOVANOV, BUYANOV, and VINNIK.

2 55. The Mt. Gox exchange was the subject of a series of computer intrusions and resulting  
3 thefts between approximately September 2011 and May 2014. Several hundred millions dollars' worth  
4 of bitcoin was stolen, including from numerous customers in the U.S. and within the Northern District of  
5 California. After the thefts, some approximately 530,000 of the bitcoin (worth hundreds of millions of  
6 dollars) stolen from Mt. Gox was deposited into wallets at three different digital currency exchanges: (i)  
7 BTC-e; (ii) Trade Hill, another exchange based in San Francisco; and (iii) back into Mt. Gox into a  
8 different Mt. Gox wallet.  
9

10 56. Of this 530,000 bitcoin,<sup>7</sup> 300,000 of it was sent directly to three separate BTC-e  
11 accounts: "Vamnedam," "Grmbit," and "Petr." These accounts were all linked to each other.  
12

13 57. Meanwhile, blockchain analysis reveals that the stolen Mt. Gox funds that went to Trade  
14 Hill and back into the other Mt. Gox account were controlled by a user who also controlled a BTC-e  
15 account called "WME." At all times relevant to this Indictment, defendant VINNIK exercised control  
16 over the BTC-e "WME" account.

17 58. The "Vamnedam," "Grmbit," "Petr," and "WME" accounts were each directly linked to a  
18 variety of different BTC-e administrative accounts, accounts for which only BTC-e administrators  
19 and/or operators would have had access.

20 59. At least two of the same individuals who were managing and operating BTC-e,  
21 defendants NIKONOROV and BUYANOV, controlled and operated the "Vamnedam" account. In  
22 addition, between approximately August 2013 and November 2015, defendants NIKONOROV,  
23 BUYANOV, and GOLOVANOV received direct payments from the "Vamnedam" account to their own  
24 personal digital currency accounts at another digital currency exchange, Bitstamp. These bitcoins were  
25 then exchanged into fiat currency and sent to NIKONOROV's, BUYANOV's, and GOLOVANOV's  
26

27  
28 <sup>7</sup> The amount of bitcoin stolen from Mt. Gox accounted for just under half of the total thefts that Mt. Gox suffered.



1 personal bank accounts in Cyprus and Latvia.

2 60. In other words, in addition to being BTC-e's operators, administrators, and benefactors,  
3 defendants NIKONOROV, BUYANOV, GOLOVANOV, and VINNIK used BTC-e accounts to launder  
4 a significant amount of bitcoin stolen from the Mt. Gox exchange. Of course, this was just one of many  
5 examples of criminal funds that were laundered through BTC-e as part of the defendants' broader  
6 conspiracy to commit money laundering.

### 7 8 STATUTORY ALLEGATIONS

9 COUNT ONE: (18 U.S.C. § 1960 – Operation of an Unlicensed Money Transmitting Business)

10 61. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein  
11 as if set forth in full.

12 62. Title 18, United States Code, Section 1960, makes it a crime to operate an unlicensed  
13 money transmitting business. The term money transmitting includes “transferring funds on behalf of the  
14 public by any and all means including but not limited to transfers within this country or to locations  
15 abroad by wire, check, draft, facsimile, or courier.” This statute makes it a violation to conduct a  
16 “money transmitting business” if the business is not registered as a money transmitting business with the  
17 Secretary of the Treasury as required by a separate statute, Title 31, United States Code, Section 5330  
18 and federal regulations pursuant to that statute.

19 63. The regulations specifically apply to foreign-based money transmitting businesses doing  
20 substantial business in the United States. See C.F.R. §§ 1010.100(ff)(5), 1022.380(a)(2).

21 64. From in or about 2011, up to and including in or about May 2016, both dates being  
22 approximate and inclusive, in the Northern District of California and elsewhere, the defendants,  
23

24 BTC-e a/k/a CANTON BUSINESS CORPORATION,  
25 ANDREY NIKONOROV,  
26 STANISLAV GOLOVANOV,  
27 ALEXANDER BUYANOV, and  
28 ALEXANDER VINNIK,

and others known and unknown to the Grand Jury, knowingly conducted, controlled, managed,

1 supervised, directed, and owned all and part of a money transmitting business affecting interstate and  
 2 foreign commerce, i.e. BTC-e, which (i) failed to comply with the money transmitting business  
 3 registration requirements set forth in Title 31, United States Code, Section 5330, and the regulations  
 4 prescribed pursuant to that statute, including 31 C.F.R. Sections 1010.100(ff) (5) and 1022.380(a)(2);  
 5 and (ii) otherwise involved the transportation and transmission of funds known to the defendants to have  
 6 been derived from a criminal offense and intended to be used to promote and support unlawful activity.

7 All in violation of Title 18, United States Code, Sections 1960 & 2.

8  
 9 COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

10 65. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein  
 11 as if set forth in full.

12 66. From in or about July 2011, through in or about May 2016, both dates being approximate  
 13 and inclusive, within the Northern District of California, and elsewhere, the defendants,

14  
 15 BTC-e a/k/a CANTON BUSINESS CORPORATION,  
 16 ANDREY NIKONOROV,  
 17 STANISLAV GOLOVANOV,  
 ALEXANDER BUYANOV, and  
 ALEXANDER VINNIK,

18 and others known and unknown to the Grand Jury, willfully and knowingly did combine, conspire,  
 19 confederate, and agree together and with each other to knowingly conduct and attempt to conduct  
 20 financial transactions affecting interstate commerce and foreign commerce, which transactions involved  
 21 the proceeds of specified unlawful activity, that is, operation of an unregistered money transmitting  
 22 business in violation of Title 18, United States Code, Sections 1960; computer hacking and intrusions in  
 23 violation of Title 18, United States Code, Section 1030; identity theft in violation of Title 18, United  
 24 States Code, Section 1028; interstate transportation of stolen property in violation of Title 18, United  
 25 States Code, Section 2314; theft of government proceeds and extortion in violation of Title 18, United  
 26 States Code, Sections 641 and 1951; and narcotics trafficking in violation of Title 21, United States  
 27 Code, Section 841; with the intent to promote the carrying on of the specified unlawful activity, and that  
 28

1 while conducting and attempting to conduct such financial transactions, knew that the property involved  
 2 in the financial transactions represented the proceeds of some form of unlawful activity, in violation of  
 3 Title 18, United States Code, Section 1956(a)(1)(A)(i).

4 All in violation of Title 18, United States Code, Section 1956(h).

5  
 6 FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

7 67. All of the allegations contained in this Indictment are re-alleged and by this reference  
 8 fully incorporated herein for the purpose of alleging forfeiture pursuant to the provisions of Title 18,  
 9 United States Code, Section 982(a)(1).

10 68. Upon a conviction for the offenses alleged in Counts 1 through 2 of this Indictment, the  
 11 defendants,

12 BTC-e a/k/a CANTON BUSINESS CORPORATION,  
 13 ANDREY NIKONOROV,  
 14 STANISLAV GOLOVANOV,  
 15 ALEXANDER BUYANOV, and  
 16 ALEXANDER VINNIK,

17 shall forfeit to the United States pursuant to 18 U.S.C. § 982(a)(1) any property, real or personal,  
 18 involved in those offenses or any property traceable to such offenses, including, but not limited to, the  
 19 following:

20 If any of the aforementioned property, as a result of any act or omission of the defendants

- 21 a. cannot be located upon the exercise of due diligence;
- 22 b. has been transferred or sold to, or deposited with, a third person;
- 23 c. has been placed beyond the jurisdiction of the Court;
- 24 d. has been substantially diminished in value; or
- 25 e. has been commingled with other property that cannot be divided without  
 26 difficulty;

27 any and all interest the defendant has in other property shall be vested in the United States and  
 28 forfeited to the United States pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b)(1).

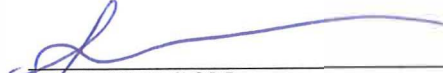
All in violation of Title 18, United States Code, Section 982(a)(1) and Rule 32.2 of the Federal

Rules of Criminal Procedure.

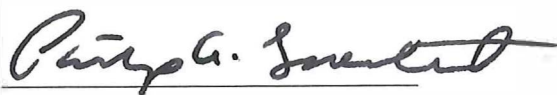
DATED:

5/31/16

A TRUE BILL

  
FOREPERSON

BRIAN J. STRETCH  
United States Attorney



DAVID CALLAWAY  
Chief, Criminal Division  
PHILIP GUENTERT  
Deputy Chief, Criminal Division

(Approved as to form: )

KATHRYN HAUN  
WILLIAM FRENTZEN  
Assistant U.S. Attorneys

INDICTMENT



United States District Court  
Northern District of California

CRIMINAL COVER SHEET

**Instructions:** Effective January 3, 2012, this Criminal Cover Sheet must be completed and submitted, along with the Defendant Information Form, for each new criminal case. Please place this form on top of the Defendant Information Form.

Case Name:

USA v. BTC-E A/K/A CANTON BUSINESS CORPORATION, et. al.

Case Number:

C R 16 0227

Total Number of Defendants:

1 \_\_\_\_\_ 2-7 ☒ 8 or more \_\_\_\_\_

Is This Case Under Seal?

Yes ☒ No \_\_\_\_\_

Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326?

Yes \_\_\_\_\_ No ☒

Venue (Per Crim. L.R. 18-1):

SF ☒ OAK \_\_\_\_\_ SJ \_\_\_\_\_

Is this a death-penalty-eligible RICO Act gang case?

Yes \_\_\_\_\_ No ☒

Assigned AUSA (Lead Attorney):

Kathryn Haun

Comments:

Date Submitted:

05/31/2016